All Computers Are Beschlagnahmt

Wie schütze ich meine Daten vor Einsicht durch die Behörden?

Version 1.1.0
Datum 18.03.2020

Weitergabe und Druck ausdrücklich erwünscht.

Bei Änderungen bitte kenntlich machen dass es sich nicht um die Originalversion des Dokuments handelt.

V.i.S.d.P.: Murray Hopper, Käferstr. 23, 87455 Buggen

Kontakt: beschlagnahmt@riseup.net
PGP Key auf Anfrage. Fingerprint:
96D2 D925 9050 EFBD C187
5334 A02F 772C 7A0E 353F

Lizenziert unter WTFPL

Inhalt

Einleitung
Hausdurchsuchung
Nach der Beschlagnahme
Online-Durchsuchung
Kommunikationsüberwachung
Löschen
Verschlüsseln
  Grundsätzliches
  Computer
  Handy
  Kommunikation
    Asymmetrische Verschlüsselung
    E-Mail
    PGP Fingerprints
    Messenger
    Telefonie
  Passwort
  Glaubhafte Abstreitbarkeit
Accountsicherheit
  Passwortmanager
  Two Factor Authentication
  Phishing
Systemsicherheit
Anonymität
  Tor
  VPN
  Whonix und Tails
IMSI Catcher und Stille SMS
Opsec
Anbieter
Resümee
Links zum Thema

Einleitung

Die deutschen Behörden können deine elektronischen Geräte beschlagnahmen, auslesen und deine Kommunikation überwachen. Das passiert gar nicht so selten. Sei vorbereitet wenn der Fall eintritt.
Mit ein paar Tricks kannst du dafür sorgen dass die ganze Aktion zwar nervig ist, aber erfolglos bleibt. Denn wer will schon, dass der Staat in persönlichen Daten rumschnüffelt?

Auf den nächsten Seiten bekommst du einige Anhaltspunkte wie du dich schützen kannst auch ohne ein Computernerd zu sein.
Lieber jetzt ein wenig Arbeit investieren und dafür bleiben später deine Daten für die Cops tabu.

Hausdurchsuchung

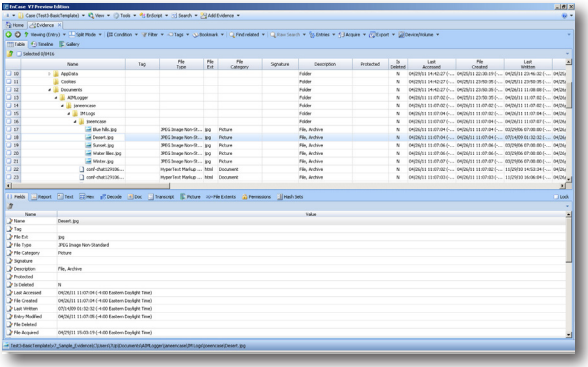
Guten Morgen Sonnenschein! Es ist 6 Uhr morgens und einige unfreundliche Beamt*innen stehen in deiner Wohnung und erklären dir dass sie nun eine Durchsuchung durchführen werden. Du bleibst natürlich cool und rufst dir in Erinnerung wie du dich in so einer Situation verhalten solltest. [1] [2] [3]

Deinen Computer fährst du herunter, wenn du keine Zeit hast ziehst du einfach den Stecker. Dank der Verschlüsselung sind die Daten damit nach wenigen Sekunden sicher. Aus dem gleichen Grund schaltest du auch dein Handy aus, wenn du telefonieren musst kannst du es immernoch wieder anschalten oder das Festnetztelefon benutzen.
Irgendwann werden sie dann anfangen deinen Kram einzupacken. Du achtest darauf das sie sich an den Durchsuchungbeschluss halten und bist ansonsten ganz entspannt.

Nach der Beschlagnahme

Jetzt werden die Cops oder ein*e Sachverständige*r sich daran machen deine Daten auszulesen und “gerichtssicher” zu machen. Wenn du deinen Kram anständig verschlüsselt hast werden sie dabei nicht weit kommen. Andernfalls werden die Daten akribisch durchsucht. Den dabei verwendeten Forensikprogrammen entgeht kaum etwas und selbst gelöschte Daten können wiederhergestellt werden.
Auch gesperrte Handys können mit der Spezialsoftware und -hardware ausgelesen werden.
Die Funde werden mit einer Prüfsumme versehen und katalogisiert, so dass sie vor Gericht als Beweis verwendet werden können.

Wird das Verfahren irgendwann eingestellt bekommst du deine beschlagnahmten Sachen zurück. Das kann aber dauern und es soll auch schon vorgekommen sein dass Festplatten die nicht entschlüsselt werden konnten bei der Rückgabe auf einmal leer waren.



Beweissicherung mit Guidance Software EnCase

Online-Durchsuchung

Eine “Online-Durchsuchung” lässt sich weniger mit einer Hausdurchsuchung vergleichen und eher mit einem Lauschangriff. Die Behörden versuchen dabei einen Trojaner [4] auf dem Zielsystem zu installieren und so Daten und Kommunikation abzugreifen. Der Rahmen der Spionage ist dabei nicht ganz klar. So hat zum Beispiel die Firma DigiTask, der Hersteller des “Staatstrojaners”, Funktionen in die Software eingebaut die die Behörden überhaupt nicht nutzen dürften. [5] Auch die Software FinFisher der deutschen Firma Gamma Group wurde zeitweise ohne Rechtsgrundlage vom LKA Berlin lizenziert. [6] Da durch diese Überwachungsmethode Verschlüsselung umgangen werden kann ist es wichtig, dass du darauf achtest das deine Systeme sauber bleiben.
Hinweise dazu findest du im Kapitel “Systemsicherheit“.
Nette Geschichte am Rande: Die Firmen Gamma und Hacking Team wurden beide von einem Frosch namens Phineas Phisher gehackt und interne Daten über ihre Geschäfte ins Netz gestellt. [7] [8]

Kommunikationsüberwachung

Bei der Telekommunikationsüberwachung, oder kurz TKÜ hören die Behörden Kommunikation direkt beim Dienstbetreiber ab. Das kann zum Beispiel euer Handyanbieter sein, euer Internet-Provider oder euer E-Mail Service. Es können viele Daten auch im Nachhinein angefordert werden, zum Beispiel die Websites die du aufgerufen hast, die Nummern die du angerufen hast, die E-Mails die du geschrieben hast und die Privatnachrichten die du auf Facebook verschickt hast. (Vorrausgesetzt der Anbieter hat diese Daten noch gespeichert.)
Auch hier kannst du dich wieder durch verschiedene Verschlüsselungsverfahren schützen.

Um das Thema Vorratsdatenspeicherung wird aktuell noch gestritten. Momentan ist diese ausgesetzt, wie sich das in Zukunft entwickeln wird ist aber noch unklar. Halte dich am besten gelegentlich etwas auf dem Laufenden. [9]

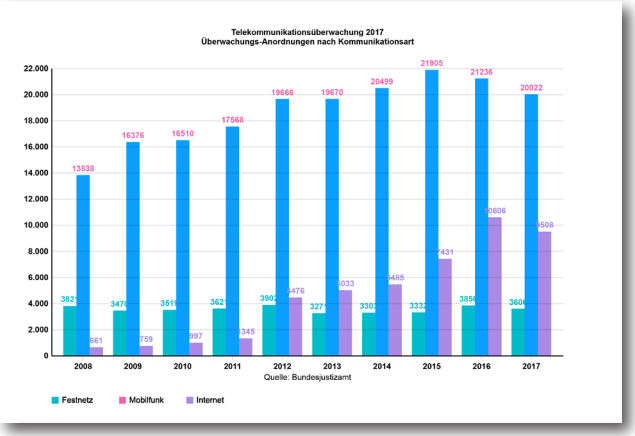
Neben solchen Anfragen bei Dritten gibt es auch noch den sogenannten “Großen Lauschangriff” also das direkte Abhören der Wohnung mit Mikrofonen. Dieser wird aber recht selten angewandt. Anzunehmen sind vielleicht 10-15 Fälle pro Jahr. Beachte das eine Hausdurchsuchung für die Cops eine gute Gelegenheit ist Wanzen zu deponieren.

Wer ebenfalls gelegentlich mithört sind die Sprachassistenten von Google, Apple und Amazon. Diese Geräte nehmen kontinuierlich ihre Umgebung auf. (Sonst könnten sie ja auch gar nicht auf ein “Hey Google” reagieren.) Aufzeichnungen von Sprachbefehlen werden auf den Servern der Anbieter gespeichert und können theoretisch auch von den Behörden angefragt werden.

Mensch sollte es sich auf jeden Fall zweimal überlegen welche Gespräche in der Gegenwart von Alexa oder einem Handy mit aktivierter Google-Sprachsteuerung geführt werden sollten.

Statistik

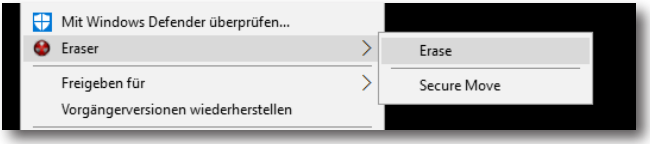
Wie oft werden eigentlich Überwachungsmaßnahmen angeordnet? Beispielhaft schauen wir uns hier mal die Statistiken von 2015 und 2017 an, welche von netzpolitik.org aufbereitet wurden. [10] [11]
Im Jahr 2015 gab es 3332 Festnetz-Überwachungen, 21906 Mobilfunküberwachungen und 7431 Internetüberwachungen. Verkehrsdatenüberwachungen, also das Sammeln von Metadaten über die Kommunikation wurde in ganzen 26265 Fällen angeordnet und die Anordnung in weiteren 899 Fällen verlängert.
Im Jahr 2017 sind diese Zahlen leicht abgesunken, aber im Vergleich noch immer ausgesprochen hoch.



Löschen

Wie wir vorhin Erfahren haben können die Cops und Sachverständige also gelöschte Daten wiederherstellen. Wie kann das angehen?
Wenn du eine Datei auf deinem Computer löschst verschwinden die Einsen und Nullen auf der Festplatte nicht automatisch. Sie werden nur zum Überschreiben freigegeben falls der Platz für was anderes gebraucht wird. Du kannst die Datei also nicht mehr sehen, aber sie lässt sich mit etwas Arbeit noch rekonstruieren. (Auch wenn du den Papierkorb bereits “geleert” hast.)
Die Lösung ist zum Glück ganz einfach. Wenn du die Daten sofort beim Löschen überschreibst kommt da keine*r mehr dran. Es gibt auch Programme die das für dich machen. [12][13][59]

Löschen mit Eraser (Win):
1. Eraser installieren (Standardinstallation)
2. Rechtsklick auf die Datei
3. “Eraser” und Unterpunkt “Erase” auswählen
4. Nochmal mit Klick auf “Yes” bestätigen
5. Warten bis die Datei verschwunden ist



Wenn dir das bei großen Dateien zu lange dauert kannst du in den Eraser-Einstellungen als Löschmethode auch “Pseudorandom Data (1 Pass)” auswählen.

Wenn du mit der Kommandozeile zurecht kommst kannst du auch „SDelete“ von Microsoft verwenden. Das ist wahrscheinlich sogar etwas gründlicher.

Löschen mit SDelete (Win):
1. SDelete installieren
2. In der CMD zum Speicherort navigieren
3. „sdelete DATEINAME“
4. Warten bis Datei verschwunden ist

Löschen mit shred (Linux):
1. wipe installieren (Paketverwaltung)
2. Im Terminal zum Speicherort navigieren
3. “`wipe -f DATEINAME`*” eingeben*
4. Warten bis die Datei verschwunden ist

Eine weitere Option für die du kein laufendes Betriebssystem brauchst ist DBAN. [14]

Diese Techniken sind nur für klassische Festplatten geeignet. Für SSDs, SD-Karten, USB-Sticks und den internen Speicher von Handys funktioniert das leider nicht so gut. Das Überschreiben schadet dem Gerät und es können trotzdem noch Daten zurückbleiben. Wenn du so einen Speicher hast kannst du dich auf den Seiten des Hersteller erkundigen ob es für das Gerät sichere Löschfunktionen gibt. Fast alle Hersteller stellen dafür Software zur Verfügung.

Ein weiteres Risiko ist das sogenannte Journaling. Das ist eine nützliche Technik um zu verhindern das Daten verloren gehen, die fast überall eingesetzt wird. Allerdings führt sie dazu das Forensiker*innen eventuell Metadaten wie Dateinamen oder sogar Dateiinhalte aus dem Journal wiederherstellen können, selbst wenn die eigentlichen Daten überschrieben wurden.

⚠ **Fallstrick beim Löschen** ⚠
Manche Systeme speichern zu Bilddateien kleine Vorschaubilder ab. Diese bleiben auch nach dem Löschen der Originaldatei erhalten.

Windows: `%userprofile%\AppData\Local\Microsoft\Windows\Explorer`

Linux: `~/.cache/thumbnails/`

Du bist mit allen Datenträgerarten auf der sicheren Seite wenn du deine Datenträger von vornherein verschlüsselst. Denn dann würde zum Wiederherstellen von Daten immer noch das Passwort benötigt werden.

Oder du arbeitest einfach gleich ohne eine Festplatte. Dazu gibt es Live-Systeme wie Tails. Du kannst dann alle Festplatten aus deinem Gerät ausbauen und das Betriebssystem von einem USB-Stick starten. Nach dem herunterfahren sind alle Daten verschwunden. Mehr dazu findest du im Abschnitt „Whonix und Tails“.

Als letzte Option bleibt immer den Datenträger physisch zu zerstören. Sei dabei ruhig gründlich und trage eine Staubschutzmaske um keinen Glas- oder Metallstaub einzuatmen, das ist wirklich sehr ungesund.

Verschlüsseln

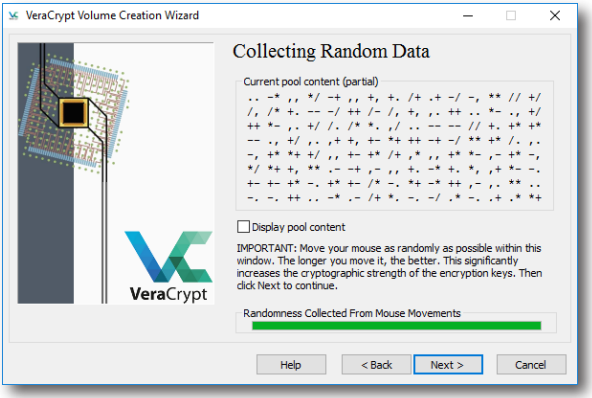
So schützt du also die Daten die du eh nicht mehr haben willst. Aber was ist mit denen die du noch brauchst?
Diese solltest du verschlüsseln. Wenn du das richtig machst haben die Behörden kaum eine Chance an die Daten heranzukommen.

Grundsätzliches
Ein Versteck ersetzt keine Verschlüsselung. Irgendwo tief in einem Ordner abgelegte Dateien werden die Behörden mit hoher Sicherheit finden. Gleiches gilt für in der Wohnung versteckte Datenträger. Effektiv schützen kannst du dich nur indem du deine Daten verschlüsselst. Wenn sie Datenträger mitnehmen ist das egal, da sie dich nicht zwingen können das Passwort herauszugeben. In den gleich folgenden Anleitungen wirst du dir an einigen Stellen ein Passwort ausdenken müssen. Bitte beachte hierfür auch den Abschnitt “Passwort”**.** Ein gutes Passwort ist für die Sicherheit deiner Daten essentiell. Wenn du Backups von deinen Daten anlegst denk daran auch diese zu verschlüsseln. Bevor du versuchst deine Geräte zu verschlüsseln lege auch eine Sicherung an, falls mal was schiefgeht.
Und noch was: Am sichersten sind die Daten die du gar nicht erst speicherst. Halte dich besonders bei heiklen Informationen an das Konzept der Datensparsamkeit.
Wenn du unbedingt Papiere aufbewahren musst tue dies in einem Umschlag der mit “Für meinen Anwalt” o.Ä. beschriftet ist.

Computer
Für deinen Computer hast du zwei grundlegende Optionen. Du kannst das gesamte System verschlüsseln, oder einen verschlüsselten Container anlegen in dem du du vertrauliche Dateien ablegst.

Systemverschlüsselung mit VeraCrypt (Win) [15][16] :
1. VeraCrypt installieren und starten
2. “Create Volume” klicken
3. “Encrypt the system partition” anwählen und “Next” klicken
4. “Normal” anwählen, “Next”
5. “Encrypt the whole drive”

6. Single- oder Multiboot auswählen. Wenn du nicht weißt worum es geht wähl einfach ersteres
7. Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
8. Passwort eingeben (siehe dazu Kapitel „Passwort“)
9. Die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann “Next”
10. “Next”
11. Entsprechend der Anweisungen eine Rescue Disk erstellen. Wenn du kein CD-Laufwerk hast kannst du auch einen USB-Stick verwenden. Mit der CD bzw. dem USB-Stick kannst du das System nicht wiederherstellen wenn du dein Passwort vergessen hast. Sie dienen nur dazu das System zu retten falls Dateien beschädigt wurden die VeraCrypt zum entschlüsseln benötigt. Du solltest den Datenträger also gut aufbewahren, wenn die Cops ihn kriegen sind deine Daten aber trotzdem noch sicher.



VeraCrypt benötigt Zufallsdaten zum verschlüsseln.

12. “1-Pass” Wipemode auswählen (Das kennen wir schon vom Löschen)
13. “Test” klicken. Der Rechner wird nun neustarten und du kannst dich das erste mal mit deinem Passwort anmelden. Wenn ein “PIM” verlangt wird drücke einfach Enter. Wenn alles funktioniert hat kann es weitergehen.
14. VeraCrypt sollte sich automatisch gestartet haben. Auf den Button “Encrypt” klicken
15. Notfallanweisungen lesen, ggf. drucken und mit “Ok” bestätigen
16. Abwarten bis alles verschlüsselt ist

Bei größeren Windows-Updates wird es Probleme geben wenn die Festplatte komplett verschlüsselt ist. Das Update schlägt dann fehl und muss zurückgerollt werden. Wenn du Pech hast kann dadurch sogar deine verschlüsselte Partition beschädigt werden oder der Rechner kann nicht mehr starten. Seit Version 1.23 von VeraCrypt gibt es eine Technik mit der du trotzdem ein solches Update durchführen kannst. Versuche auf keinen Fall größere Updates ohne diese Maßnahmen einzuspielen.

Windows Upgrade eines verschlüsselten Systems [17]:
1. Erstelle ein Installationsmedium mit dem Media Creation Tool von Microsoft
*2. Öffne eine Kommandozeile (Einfach im Startmenü “cmd” eingeben und mit Rechtsklick als Administrator*in ausführen)*
3. Navigiere in das Verzeichnis mit der setup.exe das du in Schritt 1 erstellt hast
4. Führe den Befehl
`.\setup.exe /ReflectDrivers “C:\Program Files\VeraCrypt” /PostOOBE C:\ProgramData\VeraCrypt\SetupComplete.cmd`
aus. (Alles in einer Zeile)
5. Folge den Anweisungen auf dem Bildschirm

Sollte dir das wirklich viel viel zu kompliziert sein kannst du auch schauen ob deine Windows Version “Bitlocker” mit dabei hat. Das ist das Verschlüsselungs-Programm von Microsoft. Es ist einfacher zu bedienen, allerdings ist es sehr wahrscheinlich das dort Hintertüren eingebaut wurden. Allgemein kann VeraCrypt da deutlich mehr Vertrauen entgegen gebracht werden, aber bevor du stattdessen gar keine Verschlüsselung benutzt verwende lieber Bitlocker.

Das war die Systemverschlüsselung. Alternativ kannst du auch einen Container erstellen und deine Daten darin ablegen anstatt das ganze System zu verschlüsseln. Dann musst du natürlich darauf achten keinerlei kritische Daten außerhalb des Containers zu belassen, was nicht immer ganz einfach ist.

Container mit VeraCrypt (Win, Linux) [18] :
1. VeraCrypt installieren und starten
2. “Create Volume” klicken
3. “Create an encrypted file container” anwählen und “Next” klicken
4. “Standard VeraCrypt volume”
5. Einen Speicherort und Dateinamen für deinen Container auswählen, den Haken bei “Never save history” belassen
6. Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
7. Größe des Containers festlegen
8. Passwort eingeben (siehe dazu Kapitel „Passwort“)
9. Ein Dateisystem auswählen (FAT ist in Ordnung) und die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann “Format”
10. Abwarten bis die Erstellung abgeschlossen ist und mit “Exit” das Programm verlassen

Container mit VeraCrypt öffnen:
1. VeraCrypt starten
2. Freien Laufwerksbuchstaben auswählen
3. “Select File” und die Containerdatei auswählen
4. “Mount”
5. Passwort eingeben und “Ok” klicken

Wie erwähnt bringen viele Linux-Betriebssysteme bereits Verschlüsselungsmechanismen mit. Zwischen den Verschiedenen Linux-Distributionen gibt es einige Unterschiede. Meistens ist es am einfachsten die Verschlüsselung direkt bei der Installation zu aktivieren. Beispielhaft stehen hier die Schritte für Ubuntu, unter “Mehr zum Thema” findest du aber auch Anleitungen für andere Distributionen und Möglichkeiten auch ohne Neuinstallation ein verschlüsseltes System zu bekommen. [19]

Systemverschlüsselung bei der Installation (Ubuntu):
1. Installationsprozess starten
2. Im Fenster “Art der Installation” einen Haken bei “Encrypt the new Ubuntu installation for security” setzen und weiter zum nächsten Schritt
3. Passwort eingeben (siehe dazu Kapitel „Passwort“)
4. Haken bei “Overwrite empty disk space” setzen
5. Mit “Install Now” die eigentliche Installation starten

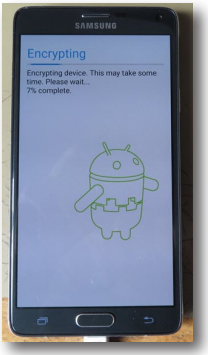
Bedenke das diese Verfahren umgangen werden können indem in deine Wohnung eingedrungen wird und ein Keylogger installiert wird. Das ist ein kleines Gerät am USB Anschluss oder eine Software welche die Tastatureingaben mitschneidet. Statte also dein UEFI und ggf. deinen Bootloader mit einem Passwort aus [20] und prüfe immer mal wieder den Anschluss deiner Tastatur auf Unregelmäßigkeiten.

Handy

Die meisten Smartphones unterstützen ebenfalls eine Systemverschlüsselung.

Das funktioniert unterschiedlich gut und auf jedem Gerät ein wenig anders. Den genauen Weg für dein Gerät recherchierst du am besten selber, aber im großen und ganzen läuft das so ähnlich wie beim Computer. [21] Du lädst das Handy auf und lässt es am Ladegerät, suchst im Einstellungsmenü die Option zum verschlüsseln, gibst zweimal dein gewünschtes Passwort ein und wartest bis der Prozess abgeschlossen ist. Teilweise muss nochmal explizit angewählt werden das auch die externe Speicherkarte verschlüsselt werden soll. Grundsätzlich ist das alles auch genau so sicher wie auf dem Computer, aber besonders ältere Geräte die nicht mehr mit Updates versorgt werden stellen ein zusätzliches Risiko dar.

Trotz Verschlüsselung ist es also vernünftig zu Aktionen nur ein billiges Zweit-Handy mitzunehmen auf dem keine persönlichen Daten gespeichert sind. Auch eine SIM-Karte die nicht mit deinem Namen verknüpft ist, ist dabei eine gute Idee.



⚠ Fallstrick beim Handy-Verschlüsseln ⚠
Wenn du ein Smartphone von Samsung hast wird das mit der Verschlüsselung leider etwas unpraktisch. Normalerweise musst du dein Entschlüsselungspasswort nur beim Starten des Geräts eingeben. Während es an ist kannst du dann deinen normalen Lockscreen benutzen. Samsung zwingt dich aber das Passwort jedes mal einzugeben wenn du den Bildschirm entsperren willst. Ziemlich unpraktisch und verleitet dazu ein unsicheres Passwort zu benutzen.

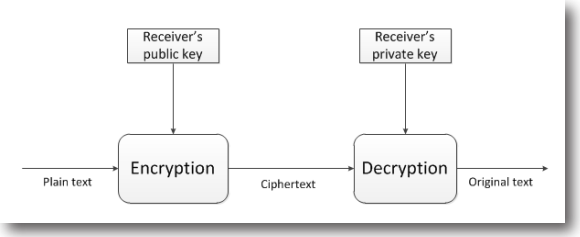
Kommunikation
Wenn du eine Nachricht über das Internet versendest wird sie viele Stellen durchlaufen bis sie am Ziel angekommen ist. Vielen davon musst du ohne Verschlüsselung einfach vertrauen das sie deine Daten schützen und sich im Zweifel auch gegen Behördenanfragen zur Wehr setzen. Das machen aber leider viele nicht. Zum Beispiel ist bekannt das 1&1 zu denen auch GMX und Web.de gehören ohne große Rückfragen gespeicherte Daten weitergeben. Aber auch bei kleineren Anbietern solltest du dich nicht darauf verlassen dass die Betreiber*innen für dich in den Knast gehen werden wenn sie eine Anfrage bekommen. Die Lösung ist auch hier wieder Verschlüsselung.

Asymmetrische Verschlüsselung
Was wir gerade für die Verschlüsselung unserer Geräte verwendet haben war eine traditionelle symmetrische Verschlüsselung. Das bedeutet das die Person an die Daten kommt die das Passwort hat. Für Kommunikation ist das etwas unpraktisch, da so das Passwort zwischen allen Kommunikationsteilnehmer*innen auf einem sicheren Kanal ausgetauscht werden muss bevor kommuniziert werden kann. Das ist umständlich und bringt das

Risiko mit sich, dass das Passwort beim Austausch abgefangen wird. Dieses Problem wird mit asymmetrischer Verschlüsselung gelöst. Bei dieser haben unsere Kommunikationsteilnehmer*innen Alice und Bob je einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird nur zum *verschlüsseln* verwendet, der private Schlüssel wird nur zum *entschlüsseln* verwendet.

Alice und Bob?
Alice und Bob sind die “Anna und Arthur” der Kryptografie, In unserem Beispiel wollen die beiden miteinander kommunizieren ohne dass Mallory mitlesen kann.

Ein privater und ein öffentlicher Schlüssel bilden ein Schlüsselpaar. Eine Nachricht die mit Bobs öffentlichem Schlüssel verschlüsselt wurde kann nur mit seinem privatem Schlüssel entschlüssselt werden. Selbst Alice die die Nachricht verschlüsselt hat kann die Verschlüsselung nicht rückgängig machen, denn nur Bob kennt den privaten Schlüssel.



Dieses Verfahren wird fast überall verwendet wo ohne einen sicheren Kanal zum Passwortaustausch kommuniziert werden muss. Es ist auf den ersten Blick etwas kompliziert, funktioniert aber gut.

E-Mail
Verschlüsselte Kommunikation mit GPG4Win und Kleopatra (Win) [22]:

Installieren und eigene Schlüssel erstellen:
1. GPG4Win installieren (bei der Komponentenauswahl "Kleopatra" ausgewählt lassen
2. "New Key Pair" klicken
3. Optional Name und Mail vergeben
4. "Create" klicken
5. Passwort vergeben (siehe dazu Kapitel „Passwort")
6. Während der Erstellung die Maus zufällig über den Bildschirm bewegen (das benötigt der Algorithmus als Zufallswert, wir kennen das schon von VeraCrypt)

Eigenen öffentlichen Schlüssel rausfinden:
Diesen kannst du anderen Leuten geben damit sie dir verschlüsselte Mails schreiben können
1. In Hauptfenster den neu erzeugten Eintrag klicken
2. "Export" klicken
3. Gesamten Inhalt des Fensters kopieren
4. In einem Texteditor alle Zeilen die mit "Comment" beginnen entfernen, die Leerzeilen ebenso
5. Der restliche Text ist dein öffentlicher Schlüssel

Eine Nachricht verschlüsseln:
1. Öffentlichen Schlüssel der Person der du schreiben willst in die Zwischenablage kopieren
2. In Kleopatra auf "Extras" - "Clipboard" - "Import Certificate" klicken
3. Auf "No" klicken
4. Auf "Notepad" wechseln und die Nachricht eingeben
5. Im Anschluss auf den anderen Tab wechseln
*6. Alle 3 Häkchen sollen aktiviert sein, die oberen sollen deinen eigenen Schlüssel enthalten, im unteren gibst du den*die Empfänger*in ein.*

(Deren Schlüssel haben wir vorhin importiert, der ist nun auf der Hauptseite zu finden)
7. “Sign/Encrypt Notepad” klicken
8. Passwort eingeben
9. Im Tab “Notepad” sollte jetzt etwas stehen was mit “BEGIN PGP MESSAGE” anfängt und mit “END PGP MESSAGE” aufhört
10. Kopiere den gesamten Inhalt des Textfeldes und pack den in die E-Mail die du versenden willst. Die andere Person wird ihn entschlüsseln können

Eine Nachricht entschlüsseln:
1. Empfangene Nachricht in die Zwischenablage kopieren
2. “Notepad” auswählen
3. Nachricht einfügen
4. “Decrypt Notepad” klicken
5. Wenn die Nachricht mit deinem öffentlichen Schlüssel erstellt wurde kannst du sie nun lesen

> ⚠ **Fallstrick beim Verschlüsseln von E-Mails** ⚠
> Empfänger*in und Betreff einer E-Mail werden nicht verschlüsselt werden. Wähle also einen neutralen Betreff der keinen Rückschluss auf den Inhalt der Nachricht zulässt. Gegebenfalls sollten auch die E-Mail-Adressen der Kommunikationsteilnehmer*innen neutral sein, also frei von Hinweisen auf die reale Person.

Ja. das ist schon etwas umständlich. Wenn du PGP öfters nutzen willst kannst du auch ein Plugin in deinem E-Mail Programm installieren. Im Folgenden ist das mal für Thunderbird erklärt, sowas gibt es aber für die meisten E-Mail Programme. Beachte aber auch dass es etwas sicherer ist das stattdessen von Hand zu machen.

Verschlüsselte Kommunikation mit Thunderbird und Enigmail (Win & Linux) [23][24]:

1. Thunderbird installieren und mit deinem E-Mail-Konto verbinden

2. GPG (Linux) oder GPG4Win (Windows) installieren

3.Mit dem Thunderbird Addon-Manager Enigmail installieren

4. Thunderbird neustarten

5. Im Setup Wizard “Standard Configuration” auswählen und den Schritten folgen

6. Bei der Schlüsselerstellung die gewünschte E-Mail adresse aus der Liste auswählen

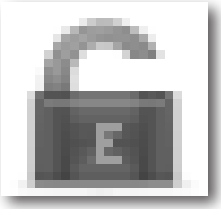
7. ggf. Passphrase eingeben

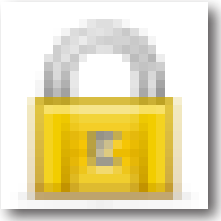
8. Warten bis die Schlüssel generiert wurden

9. Schlüssel können über das Menü “Enigmail -> Key Management” importiert und exportiert werden.

10. An dich gerichtete verschlüsselte Nachrichten werden beim Empfang automatisch entschlüsselt

11. E-Mails die du schreibst sollten automatisch verschlüsselt werden sofern du den entsprechenden öffentlichen Schlüssel importiert hast. Achte auf das Schloss Symbol über der E-Mail.





Verschlüsselte Kommunikation mit GPG (Linux):

Eigene Schlüssel erstellen
1. gpg installieren (Paketverwaltung)
2. Im Terminal “gpg --gen-key” ausführen
3. Einen beliebigen Namen eingeben
4. Optional E-Mail eingeben
5 Mit “O” bestätigen
6. Optional Passphrase eingeben

Eigenen öffentlichen Schlüssel rausfinden:
1. “`gpg --armor --export NAME`” im Terminal ausführen (Mit dem Namen der im vorherigen Schritt eingegeben wurde)
2. Schlüssel kopieren

Eine Nachricht verschlüsseln:
1. Öffentlichen Schlüssel der Person der du schreiben willst in einer Textdatei speichern
2. “`gpg --import DATEINAME`“ ausführen
3. Deine Nachricht in einer Textdatei speichern
4. “`gpg -e --armor -r ADRESSE DATEINAME`” dabei ist Adresse der Name oder die E-Mail Adresse die zu dem Schlüssel gehört den du gerade gespeichert hast
5. Im gleichen Verzeichnis sollte nun eine Datei mit der Endung .asc liegen, die enthält deine verschlüsselte Nachricht.

Eine Nachricht entschlüsseln
1. Verschlüsselte Nachricht in einer Datei speichern
2. “`gpg --decrypt DATEINAME`” ausführen

PGP Fingerprints
Während du Schlüssel erstellst oder importierst werden dir immer wieder die „Fingerprints“ der Schlüssel ange zeigt. Was ist das eigentlich? Der Name „Fingerprint“ ist

schon ziemlich sprechend. Jeder Schlüssel hat einen Fingerprint der nur zu diesem Schlüssel gehört. Wenn du einen Schlüssel aus dem Internet bekommst, zum Beispiel weil die Person ihn dir per klartext E-Mail geschickt hat, dann kannst du dir nicht sicher sein ob das auch wirklich der richtige Schlüssel ist. Vielleicht hat auch eine Behörde die Leitung abgehört und den echten Schlüssel durch einen Schlüssel ersetzt mit dem sie das Gespräch mitlesen kann. Deswegen gibt es diesen kurzen Fingerprint. Du und die andere Person können über einen sicheren Kanal die Fingerprints vergleichen und so feststellen ob beide den richtigen Schlüssel haben, die Kommunikation also sicher ist. Das kann zum Beispiel bei einem Treffen in der echten Welt passieren, oder der Fingerprint kann in einer Zeitung abgedruckt worden sein. Wenn du den Fingerprint einfach nur per Mail bekommen hast oder auf der Website der anderen Person gefunden hast dann bringt das natürlich nichts. Dort könnte wieder jemand „auf der Leitung sitzen“ und den Fingerprint durch eine Fälschung austauschen.

Messenger

Wesentlich einfacher bedienbar als PGP/GPG sind Messenger Apps auf dem Handy. Die allermeisten davon haben mittlerweile eine Ende-Zu-Ende Verschlüsselung. Natürlich ist das dann wieder eine Vertrauensfrage. WhatsApp ist sicherlich nicht immer die beste Wahl, es gehört zu Facebook und dort wird regelmäßig mit den Behörden kooperiert. Auch Telegram ist teilweise recht intransparent. Vor allem lädt es zu heftigen Bedienfehlern ein, da die Chats standardmäßig nicht Ende-zu-Ende verschlüsselt sind. [25] Warum ein Anbieter für “sichere” Kommunikation Nutzer*innen so einem Risiko aussetzt ist nicht ganz klar. Daher sollte Telegram nicht genutzt werden. Stattdessen wird von vielen die App “Signal” empfohlen, welche ganz anständige Sicherheits-

Standards hat. [26] In der App kannst du auch einstellen das Nachrichten nach einiger Zeit, zum Beispiel nach einem Tag, automatisch gelöscht werden. Wenn du auf deinem Handy verschlüsselt kommunizieren willst ist Signal der einfachste Weg. Weitere Alternativen sind „Tox“ und „Wire“ [63] [64] Eine weitere Alternative ist Jabber/XMPP welches keine zentralen Server besitzt und eher so wie E-Mail funktioniert, nur eben als Messenger und mit besserer Sicherheit. [27] Lad dir einfach die App “aTalk“ [54] oder „Conversations“ [60] runter und registriere einen Account bei einem Anbieter, so wie du es auch für eine neue E-Mail Adresse tun würdest. Eine Liste findest du im Kapitel “Anbieter”. Um eine höhere Sicherheit zu haben solltest du in den Einstellungen prüfen ob „OMEMO“ aktiviert ist. OMEMO ist sowas wie der Nachfolger von OTR und erweitert das XMPP Protokoll um Ende-Zu-Ende-Verschlüsselung. Im Gegensatz zu PGP hat OMEMO einige Vorteile, zum Beispiel die sogenannte „Forward Secrecy“ durch die Angreifer alte aufgezeichnete Nachrichten nicht entschlüsseln können, selbst wenn sie irgendwann später in den Besitz des Schlüssels kommen. Signal und Jabber/XMPP kannst du beide auch auf dem Computer nutzen. (Signal muss dafür aber trotzdem mit einer Telefonnummer registriert worden sein.) [61] SMS Nachrichten solltest du genau wie Telegram nicht für kritische Kommunikation nutzen, SMS hat keine Verschlüsselung.

Wenn du Apps auf deinem Gerät installierst vergewissere dich das du auch eine echte Version bekommen hast und keine Schadsoftware. Der einfachste Weg ist die Verwendung eines App-Stores. Auf vielen Android Geräten ist schon der Google PlayStore installiert, eine gute Alternative dazu, die auch ohne Google Account funktioniert, ist F-Droid. Die Apps dort sind alle kostenlos und Open Source. aTalk und Conversations kannst du ebenfalls dort finden. [62] Signal gibt es leider nur im PlayStore oder direkt auf der Website.

Telefonie
Genau wie SMS verfügen Telefongespräche über keine sichere Verschlüsselung. Es mag für eine Privatperson nicht ohne weiteres möglich sein ein Telefongespräch abzuhören - so viel Crypto ist dann doch da - aber für staatliche Akteure oder deinen Handyanbieter ist das ganze kein Problem. Auch kommerzielle Anbieter von Internettelefonie wie Skype sind keine verlässliche Lösung. Allerdings kannst du mit der bereits erwähnten App Signal, oder auch mit Tox oder Wire, verschlüsselt über das Internet telefonieren. Wenn du auf mobile Nutzung verzichten kannst könnte auch Jitsi [65] eine Option sein. Und damit keine Missverständnisse aufkommen: im aktivistischen Kontext ist von Telefonaten über Festnetz genau so abzuraten wie von Telefonaten mit dem Handy.

An dieser Stelle auch ein Hinweis zu alten Tastenhandys: Die Nutzung solcher Geräte kann durchaus Sinn machen. Bewegungsprofile können damit nur ungenau über Funkzellenabfragen erstellt werden und nicht so präzise wie bei einem Gerät mit GPS-Modul, es liegen weniger Daten auf dem Gerät vor und dadurch das keine Apps oder auch nur ein komplexes Betriebssystem vorhanden sind ist auch die Angriffsoberfläche deutlich geringer. Auf der anderen Seite ist es aber auch nicht möglich den Inhalt des Geräts oder die getätigte Kommunikation zu verschlüsseln. Selbst die ohnehin unsichere Verschlüsselung durch das Mobilfunknetz ist bei diesen Geräten oft noch schlechter. Wenn du dir über diese Punkte bewusst bist und andere Vorteile für dich überwiegen kannst du ein Tastenhandy benutzen, aber falle nicht auf den Trugschluss rein, das Gerät wäre grundsätzlich sicherer nur weil es keinen großen Touchscreen hat.

Zivile Handfunkgeräte können über Verschlüsselung verfügen, in der Praxis ist das aber meistens nicht der Fall.

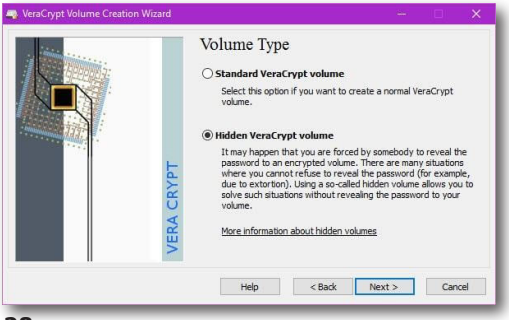
Passwort

Das Passwort ist bei all diesen Verschlüsselungsmethoden ein wichtiger Bestandteil. Im Regelfall ist es das Schwächste Glied in der Kette und die Sicherheit deiner Verschlüsselung hängt davon ab dass du ein sicheres Passwort gewählt hast, und es schaffst dieses vor den Ermittlungsbehörden geheim zu halten. Also erstmal grundlegend: Das Passwort darf nirgendwo notiert werden, es darf nichts mit dir oder deinem Umfeld zu tun haben und außer dir darf es keine*r wissen. Es muss lang sein, das heißt am besten mehr als 20 Zeichen lang, es sollte nicht aus irgendeinem einfachen Satz bestehen und du solltest definitiv *ein* Passwort für *einen* Anwendungszweck haben. Keine Mehrfachverwendungen. Es gibt verschiedene Meinungen dazu wie ein sicheres Passwort aussehen muss. Einige schwören auf wüste Sonderzeichenkombinationen, andere reihen ein paar zufällige Wörter aneinander. Wo sich aber alle einig sind ist, dass es die Länge macht. Wenn du ein Alphabet mit 26 Zeichen und ein Passwort der Länge 10 hast sind das 26^{10} mögliche Kombinationen (also 141167095653376). Wenn du dein Passwort um eine Stelle verlängerst sind es schon 26^{11} Kombinationen (also 3670344486987776). Die Arbeit die ein Computer aufbringen muss um dein Passwort zu raten wächst also mit jedem Zeichen exponentiell. Natürlich kann sich keine*r zig verschiedene elendig lange Passwörter merken. Deswegen gibt es sogenannte “Passwort-Manager” in denen du deine Passwörter abspeichern kannst. Eine Anleitung kannst du im Abschnitt “Accountsicherheit” finden. Der Grund dafür das du Passwörter nicht mehrfach verwenden solltest ist das immer wieder Passwort-Datenbanken geklaut und veröffentlicht werden. Wenn du davon betroffen bist kannst du das zum Beispiel mit haveibeenpwned.com feststellen. Dort gibst du deine E-Mail Adresse ein und die Seite zeigt dir ob du in einem der bekannten Datensätze auftauchst.

Glaubhafte Abstreitbarkeit

Als Beschuldigte*r in einem Prozess kannst du dich auf dein Aussageverweigerungsrecht berufen um das Passwort geheim zu halten. Als Zeug*in wird das schon schwieriger. Mit der Argumentation dass du dich dadurch selbst belasten würdest und daher ebenfalls ein Aussageverweigerungsrecht hast, verrätst du möglicherweise mehr als dir lieb ist. Ein ähnliches Problem hast du wenn irgendwer versucht dir das Passwort mit Gewalt oder Erpressung zu entlocken. [28] Für solche Fälle wurde das Konzept der “Glaubhaften Abstreitbarkeit” oder “Plausible Deniability” entwickelt. [29] Dein verschlüsselter Container oder dein verschlüsseltes System haben dabei zwei verschiedene Passwörter. Eines bringt dich in dein für schützenswerte Aktivitäten genutztes System, das andere in ein harmloses “Decoy-System” in dem keine sensiblen Daten gespeichert werden. Sollte nun irgendwer versuchen dich zur Herausgabe des Passworts zu zwingen kannst du einfach das Passwort für das Decoy-System nennen. Dein Gegenüber wird sich einloggen und das falsche System durchsuchen. Das noch mehr Daten existieren kann nicht erkannt werden.

Die Software VeraCrypt die wir hier bereits angesehen haben unterstützt diese Funktion. Dort heißt das ganze „Hidden Volume“.



Um diese Funktion zu nutzen beginnst du mit einem unverschlüsselten System, installierst VeraCrypt wie zuvor beschrieben und verwendest dann die Funktion *„Create Hidden Operating System“.* Die optimale Größe der verschiedenen Partitionen sollte das Programm für dich aussuchen. Dann wird ein sogenanntes „Outer Volume“ erstellt. Dieses kannst du als weitere Sicherheitsebene betrachten, Dein Decoy-System enthält nur harmlose Daten. Dein Outer-Volume enthält Daten die einen sensiblen Eindruck machen, die du aber preisgeben kannst falls du gezwunden werden sollst die versteckten Daten zu entschlüsseln. Der heiße Scheiß liegt stattdessen aber im Hidden-Volume, dessen Passwort du nie preisgibst. (Insgesamt gibt es also drei Passwörter.) VeraCrypt hat nun also das Outer-Volume erstellt und du befüllst es mit ein paar pseudo-sensiblen Daten. Das Programm wird dir sagen wie groß die Datenmenge sein darf, damit noch genug Platz für das Hidden-Volume ist in dem deine echten Geheimnisse aufbewahrt werden. Dieses wird im nächsten Schritt erstellt. Nun haben wir also ein Outer-Volume, ein Hidden-Volume und es fehlt nur noch das Decoy-System. Auf der Partition für das Decoy-System kannst du nun einfach eine neue Windows-Installation erstellen und diese mit der normalen Systemverschlüsselung von VeraCrypt verschlüsseln. Damit hast du dein Plausible-Deniability-System erfolgreich eingerichtet.

Ja, das ist leider ziemlich kompliziert, kann dir aber in bestimmten Situationen von großem Nutzen sein. Weitere Informationen und Sicherheitshinweise findest auf der Seite von VeraCrypt. [66] Eine Anleitung zu Plausible Deniability unter Linux findest du bei LinuxBrujo. [67]
Tricks wie diese können unter Umständen helfen dich in Verhörsituationen zu entlasten, aber selbstverständlich sind sie keine Garantie dass dein Gegenüber dir glaubt und ggf. auf die Anwendung von Gewalt verzichtet.

Accountsicherheit

Passwort-Manager
Was bei einem Passwort wichtig ist haben wir erklärt. Um diese super sicheren Passwörter alle aufzubewahren hilft ein Passwort-Manager. Da es bereits zu Datenlecks bei Bezahl-Anbietern kam sollte die Wahl hierbei auf Keepass fallen, denn Keepass ist Open Source, bewährt und nicht web-basiert. Wie du trotzdem die Vorzüge von Browserintegration und geräteübergreifender Synchronisation genießen kannst weiter unten.

Passwort Management mit Keepass (Win, Linux) [30]:
Das Prinzip ist denkbar einfach. Mensch lädt sich die Anwendung herunter, erstellt eine neue Datenbank, vergibt ein Hauptpasswort und kann damit beginnen, Logindaten für Websiten zu hinterlegen. Die Datenbank ist hierbei verschlüsselt. Das heißt: solange niemensch dein Passwort knackt, bringt es der Person nichts im Besitz der Datei zu sein.

Wichtig: Das Hauptpasswort wird selbstverständlich nicht in der Datenbank hinterlegt, du musst es dir also merken und es muss sicher sein. Wähle kein Passwort, welches du schon mal verwendet hast, nutze viele Zeichen, gerne auch Sonderzeichen und Zahlen. Darüber haben wir ja gerade schonmal geredet. Solltest du nun einen neuen Eintrag in der Datenbank anlegen, ist das Passwortfeld bereits gefüllt. Lässt du dir den Inhalt anzeigen, wird dort etwas unleserliches, generiertes stehen, was allein durch diese Eigenschaft schon schwer zu knacken ist. Übernimm das bei das Passwortvergabe einfach in das Passwortfeld im Browser.
Merken muss sich das zum Glück niemensch, du hast ja das Hauptpasswort.

Datenbank synchronisieren:
Falls du bereits andere Passwortmanager genutzt hast bist du in den Vorzug gekommen, auf mehreren Geräten auf deine Anmeldedaten zugreifen zu können. Das können wir mit keepass auch, vorausgesetzt du hast einen Cloudspeicher, auf dem du die Datenbank-Datei von Keepass ablegen kannst.
Hast du das getan kannst du über *“File -> Open -> Open URL”* die URL mitsamt Zugangsdaten angeben.
Wie wir bereits wissen ist es recht unbedenklich Die Datenbank online zu lagern. Auch wenn auf deinen Cloudspeicher zugegriffen wird ist die Passwortdatenbank separat verschlüsselt.

Kee:
Um die Bedienung über den Browser zu erleichtern gibt es für Chrome und Firefox das Addon “Kee”. Dieses kann Anmeldeformulare automatisch ausfüllen, Passwörter generieren oder Anmeldedaten nach einer Registrierung in der Datenbank ablegen.

> ⚠ **Risiken abwägen** ⚠
> Da die Anmeldedaten von Keepass zum Browser gelangen müssen bietet die Verwendung von solchen Addons natürlich Schadsoftware einen zusätzlichen Angriffsvektor um die Passwörter abzugreifen, falls dein System infiziert sein sollte.

*(1. Nur Für Linux/Mac User*Innen: Installiere das Paket “mono-complete”)*
2. Erstelle im Keepass Installationsordner einen Ordner namens “Plugins”
3. Lade dir die neuste KeePassRPC.plgx Datei herunter [31] und schiebe sie in den “Plugins” Ordner
4. Starte Keepass und aktiviere das Plugin
5. Installiere das Kee Browseraddon [32]

6. Konfiguriere die Verbindung zwischen dem Browser-Addon und dem Keepass-Plugin indem du der Anleitung auf dem Bildschirm folgst
7. Wenn du ein Passwort eingibst bietet Kee dir nun an es zu speichern. Mit einem Knopfdruck kannst du gespeicherte Passwörter abrufen.

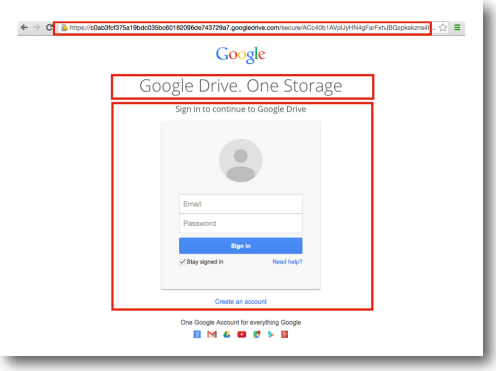
Two-Factor Authentication
Passwörter können aus verschiedenen Gründen bekannt werden. Vielleicht wurde eine Seite gehackt auf der du das Passwort verwendet hast, dir hat irgendwer beim Eingeben über die Schulter geschaut oder du hast als Passwort den Namenstag deiner Katze ausgewählt und irgendwer hat es geschafft das zu erraten. Für solche Fälle gibt es als Rettungsnetz “Two Factor Authentication” oder kurz “2FA”. Dabei installierst du eine App auf deinem Handy die dir alle 30 Sekunden einen anderen kurzen Zahlencode anzeigt. Wenn du dich jetzt zum Beispiel auf einer Website anmelden willst gibst du nicht nur dein Passwort ein, sondern auch noch den Code von deinem Handy. Ohne den Code kommt keine*r rein, das Passwort alleine reicht nicht mehr. Es werden jetzt also zwei “Faktoren” geprüft. Etwas das du weißt (das Passwort) und etwas das du besitzt (dein Handy mit der App).

Eine weit verbreitete 2FA App ist “Authy”. [33] Auf der Seite von Authy findest du auch Anleitungen für viele Anbieter wie du auf deren Seiten 2FA einrichten kannst. Eine alternative App ist “andOTP”. [34]

Damit du nicht völlig aufgeschmissen bist falls du mal dein Handy verlierst lagert Authy eine verschlüsselte Kopie deiner Datenbank auf ihrem Server. Diese kannst du mit einem Passwort abrufen. Um 2FA im Alltag zu benutzen benötigst du aber keine Internetverbindung auf dem Handy.

Phishing

Es klingt wie der billigste Trick der Welt, ist aber eine sehr verbreitete Methode um an fremde Passwörter zu gelangen. beim Phishing wird eine Seite perfekt nachgebildet und die Zielperson dazu gebracht sich auf der gefälschten Seite einzuloggen. Die Angreifer*innen können das Passwort dann lesen und sich auf der richtigen Seite einloggen. Die Nachbildungen können extrem realistisch sein, mit ein paar Tricks ist es sogar möglich das die Adresse genau gleich aussieht, zum Beispiel in dem Buchstaben aus dem kyrillischen Alphabet eingesetzt werden die wie lateinische Buchstaben aussehen. Um sicher zu gehen bedenke immer ob du die Seite auf einem vertrauenswürdigen Weg erreicht hast oder ob dir irgendwer einen langen schwer lesbaren Link geschickt hat der dich zu dieser Login-Maske gebracht hat. Am sichersten ist es wenn du Adressen immer selbst eintippst oder die Lesezeichenfunktion deines Browsers verwendest.



So könnte eine Phishing Seite aussehen. Beachte die Auffälligkeiten die hier mit Kästen markiert sind.

Systemsicherheit

Besonders weil die Behörden möglicherweise Spionage-Software auf deinem Rechner oder deinem Handy installieren wollen solltest du darauf achten diese möglichst frei von Sicherheitslücken zu halten. Daher hier nochmal ein paar Grundregeln:
- Führe regelmäßig Updates durch. Ja, das ist nervig, aber ansonsten setzt du dich einem hohen Risiko aus.
- Denke auch daran regelmäßig Updates auf deinem Router einzuspielen.
- Installiere nur Software aus vertrauenswürdigen Quellen.
- Auch wenn du Software aus einer vertrauenswürdigen Quelle installierst, zum Beispiel dem Google Play Store, frage dich immer ob du den Entwickler*innen vertraust. Das gilt sowohl für Programme auf dem Rechner, als auch für Browser-Addons und Apps.
- Lasse Windows Defender aktiviert [55]
- Nutze einen Adblocker wie uBlock Origin. Viele Werbung ist nicht nur nervig sondern auch ein Sicherheitsrisiko.
- Klicke nicht auf Links bei denen du dir nicht sicher bist wohin sie führen.
- Öffne keine E-Mail-Anhänge die du nicht erwartet hast, selbst wenn du glaubst den*die Absender*in zu kennen. Im Zweifelsfall ruf kurz an und frag ob die Person dir wirklich etwas geschickt hat.
- Wenn du Microsoft Office benutzt deaktiviere die Makro-Funktion.
- Schütze dein WLAN mit einem Passwort, ggf. ändere das vom Hersteller voreingestellte Passwort.
- Wenn du aus dem Haus gehst fahre deinen Rechner herunter anstatt ihn im Ruhezustand zu lassen

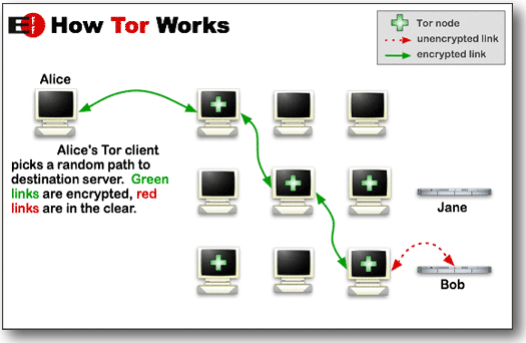
Weitere gute Tipps für Windows Nutzer*innen gibt es bei Decent Security. [35]

Anonymität

Ganz grundlegend: solltest du dich auf “verdächtigen” Seiten herumtreiben ist es immer angebracht Verschlüsslungsdienste und Anonymisierungsdienste zu verwenden. Da hast du hauptsächlich die Wahl zwischen Tor und einem VPN. Es gibt noch weitere Lösungen wie I2P oder Freenet, diese sind aber weniger verbreitet und damit auch weniger überprüft.

Tor

Bei der Verwendung von Tor (The Onion Router) [36] wird dein Traffic verschlüsselt über die Rechner freiweilliger Relay-Betreiber*innen umgeleitet, bis er dann unverschlüsselt vom letzten Knoten an die entsprechende Seite gesendet wird. Die offensichtlichen Nachteile: Tor ist langsam, es ermöglicht keine Videotelefonie und ist mit einigem Aufwand kompromitierbar. Nämlich dadurch, dass der Freund und Helfer ebenfalls im Tor-Netz unterwegs ist und eben auch als Endknoten Zugriff auf die unverschlüsselten Daten haben könnte, die du an die Website sendest. So können verschiedene Korellations- oder Timingattacken durchgeführt werden um dich zu enttarnen. Dieses Risiko ist allerdings aktuell sehr gering. Die einfachste Methode um Tor zu benutzen ist der Tor Browser. [37] Der sieht Firefox ziemlich ähnlich, leitet aber alles was im Browser passiert durch das Tor Netzwerk. Du solltest aber keine weiteren AddOns installieren, das Fenster immer auf der voreingestellten Größe lassen und keine sonstigen Einstellungen am Browser verändern. Ansonsten hebst du dich von der Masse ab und wirst möglicherweise identifizerbar. Außerdem solltest du bedenken, dass mögliche Überwacher sehen können das du Tor benutzt. Allerdings können sie nicht sehen was du mit Tor tust. Es ist also allgemein Vorsicht bei der Benutzung von Tor angesagt, wenn du keine Fehler machst solltest du damit aber komplett anonym bleiben können.



VPN

Ein VPN (Virtual Private Network) macht das mit der Anonymisierung etwas anders. Dort wird dein Internetverkehr nur an eine einzige Zwischeninstanz verschlüsselt übermittelt, nämlich den VPN-Provider. Dieser leitet dann die Daten an die entsprechenden Websites weiter. Das geht natürlich um einiges schneller, da hinter den VPNs große Konzerne stehen können, die dir den Zugang teuer verkaufen möchten und daher leistungsfähige Server haben. Dort kommt allerdings auch der Nachteil ins Spiel: ein zuverlässiges VPN ist selten kostenlos und du musst deinem Provider vertrauen keine Daten herauszugeben. Lasse also Vorsicht bei der Auswahl walten. Ein VPN das kaum etwas kostet ist vielleicht nicht immer die beste Wahl, aber ein teurer Premium Anbieter aus Deutschland oder Österreich bringt dir auch nichts, weil dieser im Zweifel mit den Behörden kooperieren wird. Wenn du einen VPN Anbieter gefunden hast der dir gefällt folge den Anleitungen des Anbieters um das VPN einzurichten. Gerade die höherpreisigen Anbieter haben meist einen guten Support. Wenn du die Einrichtung auch ohne Hilfe schaffst oder Menschen kennst die dir dabei helfen können kannst du aber etwas Geld sparen.

Im Kapitel „Anbieter“ findest du einige Empfehlungen für VPN Anbieter. Da sich die Lage in Bezug auf die Vertrauenswürdigkeit eines Anbieters aber schnell ändern kann, solltest du auch deine eigenen Recherchen anstellen, bevor du dich entscheidest. Allgemein lässt sich sagen, dass es besser ist wenn dein Anbieter auf den Seychellen sitzt anstatt in den USA, er keine falschen Versprechungen macht („wir schützen dich vor Viren“ etc.), die Möglichkeit bietet mit einer anonymen Cryptowährung wie Monero oder ZCash zu bezahlen und dir keine proprietären Clients zur Nutzung des Netzwerks andrehen will. Im besten Fall wird auf etablierte Open-Source Clients wie OpenVPN oder Wireguard gesetzt. Außerdem ist es wünschenswert wenn du für die Anmeldung keine E-Mail Adresse angeben musst, sondern eine zufällige ID zugeteilt bekommst.

Wenn du bei dem Konzept, irgendeiner Firma deine Anonymität anzuvertrauen, etwas skeptisch bist, dann hast du den richtigen Riecher. Ein VPN zur Anonymisierung zu nutzen ist besser als nichts, aber auch noch lange nicht perfekt. Hier musst du also Sicherheitsbedarf und Bequemlichkeit gegeneinander abwiegen. Je nachdem was du im Internet so machst und wer Interesse daran hat dich zu enttarnen, kann ein VPN eine ausreichende Schutzmaßnahme sein, oder nur eine kleine überwindbare Hürde für die Person oder Institution die dir an den Kragen will. Wäge diese Dinge also ab und treffe eine Entscheidung die deinem Bedrohungsmodell entspricht. Wenn du dir nicht sicher bist benutze lieber Tor. Du kannst auch im Alltag ein VPN benutzen und für bestimmte Aufgaben auf Tor umsteigen. Da musst du dann nur aufpassen, dass du zwischen deiner weniger sicheren VPN-Identität und deiner sicheren Tor-Identität keine Verbindung herstellst, zum Beispiel in dem du direkt hintereinander die gleiche Seite aufrufst, oder den gleichen E-Mail Account benutzt.

Funktionsweise eines VPN (Das mit der Firewall ist aber vor allem Marketing, uns geht es hier um die Anonymität)

Whonix und Tails

Bei Verwendung von Tor und VPN können, wie bereits erwähnt, verschiedene Dinge schiefgehen durch die deine Identität preisgegeben wird. Deswegen gibt es Betriebssysteme die wirklich allen Traffic über Tor leiten und auf andere Weise überhaupt nicht mit dem Internet reden können. Tails [38] kannst du dir herunterladen, mit dem mitgelieferten Installer auf einen USB-Stick übertragen und dann als sogennantes “Live-System” auf deinem Rechner starten. Dazu steckst du den Stick ein und startest deinen Computer neu. Wenn während dem Start eine Meldung wie “Press F12 for Boot Menu” oder so ähnlich auftaucht drücke die entsprechende Taste und wähle im folgenden Menü deinen USB-Stick aus. Nun wird anstelle deines normalen Betriebssystems Tails gestartet werden. Wenn du fertig bist kannst du den Rechner herunterfahren und den USB-Stick entfernen, dann ist alles wieder beim Alten. Das ganze hat einen Aspekt der gleichzeitig Vor- und Nachteil ist: In Tails kannst du üblicherweise keine Daten dauerhaft speichern. Nach dem Herunterfahren ist alles verschwunden.

Wenn du mehr zu Tails wissen willst lies die Broschüre der Gruppe Capulcu dazu. Die legt einen sehr hohen Sicherheitsstandard vor der wahrscheinlich für viele nicht immer praktikabel ist, enthält aber definitiv eine Menge Wertvoller Tipps. [56]
Whonix [39] funktioniert etwas anders als Tails. Für Whonix installierst du dir die Software VirtualBox [40] mit der du virtuelle Maschinen betreiben kannst. Das ist quasi ein simulierter Computer der auf deinem richtigen Computer läuft. Dann lädst du dir die Whonix Images herunter [41] und importierst diese in VirtualBox. Ja richtig gehört, es sind zwei Images. Eins davon ist das Whonix-Gateway welches die Verbindung mit dem Internet aufbaut und dafür sorgt das alles über Tor geleitet wird. Das andere ist die Whonix-Workstation. Die benutzt du um deine Arbeit zu machen. Alles was innerhalb der Workstation passiert wird über Tor geleitet werden. Dort kannst du auch Dinge speichern, denke also daran das Host-System auf dem die beiden virtuellen Maschinen laufen komplett zu verschlüsseln. Du weißt ja jetzt wie das geht. Tails und Whonix sind sehr gute Alternativen zum Tor Browser wenn dir dieser zu unsicher ist oder du noch andere Pläne hast als nur etwas im Netz zu surfen. Tails ist gut geeignet für ältere Rechner die nicht viel Leistung haben, für Whonix brauchst du schon etwas mehr, aber auf den meisten Rechnern sollte auch das noch gut funktionieren. Bedenke das du bei Whonix kein „amnesisches“ System hast, also auch Spuren hinterlässt. Nutze Whonix daher nur auf verschlüsselten Geräten. Wenn du schon etwas mehr technische Erfahrung hast und mit der Sicherheit mal so richtig auf die Kacke hauen willst dann schau dir das Betriebsystem Qubes [42] an. Dieses arbeitet mit mehreren virtuellen Maschinen und bietet neben vielen anderen Sicherheits-Features auch Ähnliche Funktionen wie Whonix an. Dafür brauchst du dann aber auch nochmal etwas mehr Leistung.

IMSI Catcher und Stille SMS

Warum wird denn eigentlich immer dazu geraten zu Demos und Aktionen nur Zweithandys mitzunehmen?
Klar, die Bullen können die eventuell dein Haupthandy wegnehmen und Daten davon gewinnen. Doch es gibt noch andere Risiken, für die du das Handy nichtmal aus der Tasche genommen haben musst. Immer wieder kommt es vor das im Umfeld von Demos IMSI-Catcher [43] aufgestellt werden. (Es ist möglich diese mit spezieller Software wie SnoopSnitch, Darshak oder AIMSICD [44][45][46] zu erkennen.) IMSI-Catcher tun so als wären sie eine normale Funkzelle im Handynetz und überreden Geräte in ihrem Umfeld dazu sich dort einzubuchen. Damit können die Bullen feststellen welche Handynummern gerade in der Umgebung sind und so die anwesenden Personen feststellen. Mit dem Gerät können auch Telefonate abgehört werden. Dazu leitet der IMSI-Catcher das Gespräch mit seiner eigenen Nummer weiter. Wird der Catcher nicht in diesem Abhörmodus betrieben sind für die Personen im Umfeld oft Anrufe komplett blockiert. Das gilt auch für Notrufe. Aus diesem Grund ist es so wichtig ein Demo-Handy mit einer anonymen SIM-Karte zu benutzen. Tust du das nicht kann deine Nummer mit dem IMSI-Catcher angezeigt werden und die Bullen müssen nur noch kurz beim Handyprovider anrufen um deinen Namen und deine Adresse herauszufinden und sie haben einen eindeutigen Beweis das du auf der Demo anwesend warst. Eine weitere Methode ist die Funkzellenabfrage, dabei sparen die Behörden sich die Arbeit mit dem IMSI-Catcher und gehen direkt zu den Betreibern der Funkzellen und lassen sich von denen eine Liste aller eingebuchten Nummern geben. Auch hier sind Fälle bekannt geworden bei denen das Verfahren auf Demos eingesetzt wurde. In Berlin gibt es mittlerweile ein “Funkzellenabfragen-Transparenz-System” mithilfe dessen du

dich nach Abschluss der Ermittlungen benachrichtigen lassen kannst falls deine Nummer bei einer Funkzellenabfrage aufgetaucht ist. [47] In anderen Bundesländern gibt es das bisher noch nicht. Das Gegenstück zum IMSI-Catcher und der Funkzellenabfrage ist die sogenannte “Stille SMS” [48], diese wird benutzt wenn die Bullen deine Nummer haben und wissen wollen wo du gerade bist. Dazu senden sie eine spezielle SMS an dein Gerät welche für dich nicht angezeigt wird. Du merkst von der ganzen Sache also gar nichts, dabei antwortet dein Handy aber mit der Funkzelle in die du gerade eingebucht bist. Anhand davon lässt sich sehr einfach dein Aufenthaltsort herausfinden. Das Bundesamt für Verfassungsschutz versendete im ersten Halbjahr 2018 ganze 103.224 stille SMS, das BKA 30.988 und die Bundespolizei 50.654. Die Landesbehörden für Verfassungsschutz und die Polizeien der Bundesländer nutzen das Verfahren ebenfalls reichlich. Es ist von deutlich mehr als einer Millionen Ortungen pro Jahr auszugehen. [49] Stille SMS können mit der bereits erwähnten App SnoopSnitch sichtbar gemacht werden.

Ein IMSI-Catcher

⚠ **Fallstrick beim Demo-Handy** ⚠
Wenn du dir ein sauberes Handy und eine anonyme Nummer besorgt hast schalte das Gerät niemals bei dir Zuhause oder an Orten an denen du dich oft aufhältst an. Damit wäre die Nummer und das Handy nicht mehr anonym. Schalte es erst an wenn du am Ort der Aktion bist. Lege die SIM-Karte nie in dein normales Handy (und andersrum). Schalte Aktionshandy und normales Handy nie am gleichen Ort ein. Überlege dir auch immer mal wieder die Nummer zu wechseln.

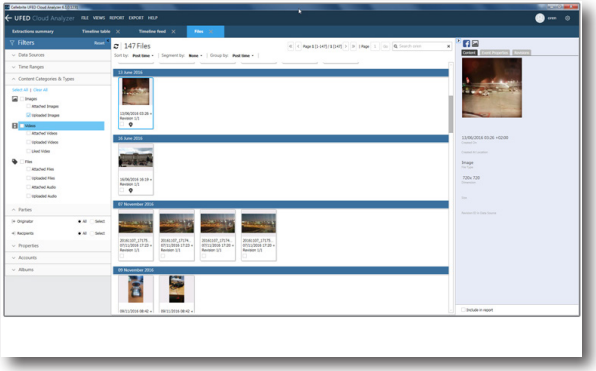
Opsec

Das Wort “Opsec” steht für “Operations security” und bezeichnet eine Reihe von Vorgehensweisen um den Gegnern kritische Informationen vorzuenthalten. Ein Teil davon sind technische Maßnahmen wie sie hier beschrieben wurden, ein zweiter sehr wichtiger Teil sind Verhaltensregeln. Mache dir bewusst welche Informationen du geheim halten möchtest und wer sich für diese interessieren könnte. Rede nicht mit der Polizei, auch nicht wenn du glaubst clever zu sein und sie mit Lügen täuschen zu können. Auch Lügen können wichtige Informationen enthalten.
Vermeide es im Kontext von Aktionen Fotos zu machen. Wenn es nicht anders geht denke daran das Foto akribisch nach Details zu durchsuchen. Verpixele Gesichter, Markenlogos auf Kleidung, Schuhe, Gebäude im Hintergrund, Stromleitungen, persönliche Gegenstände und so weiter. Prüfe auch ob dein Handy Standortdaten im Bild speichert und bereinige diese gegebenenfalls. Bei vielen Geräten ist das Speichern von Standortdaten die Standardeinstellung, vergiss diesen Schritt also auf keinen Fall. Du kannst dafür zum Beispiel die App „Scrambled Exif“ benutzen. [57]

Poste nicht in sozialen Netzwerken über deine Erlebnisse. Prahle niemals damit welchen Gruppen du angehörst, wen du kennst oder bei welchen Aktionen du dabei warst. [50]

Gehe nach einer Aktion nicht auf direktem Weg nach Hause sondern mach ruhig mal einen Umweg. Verwende während Aktionen Decknamen und Codes. [51] Wenn nötig trage bei Aktionen Handschuhe. Bedenke auch das menschliche Körper echte Dreckschleudern sind und bei jeder Gelegenheit DNA hinterlassen. Bedenke das in der Öffentlichkeit überall Kameras sind, zum Beispiel an Bahnhöfen, im Umfeld von Geschäften und Kiosks und an Polizeiwachen. Software zur Gesichtserkennung ist keine Zukunftsmusik mehr und wird bereits überall auf der Welt eingesetzt, also bedecke wenn möglich dein Gesicht. Wenn du nicht alle Tipps zur Nutzung von Demohandys akribisch befolgt hast dann lasse dein Handy am besten zuhause.

Wenn du im Internet Anonymisierungstechnologie nutzt denke daran deine Identitäten voneinander zu trennen und nicht im anonymen Kontext Dinge zu schreiben oder Logins zu nutzen die dich deanonymisieren. Wenn du diese nutzen willst dann wechsele den Kontext, zum Beispiel indem du im Tor Browser auf „New Identity“ klickst oder das VPN wechselst.
Vergiss nicht das heutzutage fast jedes Telefon ein kleiner Computer mit Mikrofon ist. Bei privaten Gesprächen schalte das Gerät aus. Am besten nimmst du den Akku raus oder lagerst es irgendwo außer Hörweite.
Das sind alles keine komplizierten Tipps, aber sie alle zu beachten ist nicht immer leicht, Reden macht nunmal Spaß. Bitte denke daran das diese Verhaltensregeln dich vor dem Knast bewahren können. Mehr dazu findest du unter den Verweisen [52] und [58].



Cellebrite UFED Cloud Analyzer zur Auswertung von Informationen aus sozialen Netzwerken

Anbieter

Hier wurde nun öfters erwähnt wie viel Vertrauen du den Menschen gegenüber bringen musst die zum Beispiel deinen Mailserver oder dein VPN betreiben. Um die Auswahl etwas leichter zu machen ist hier eine kleine Liste mit Anbietern. Recherchiere aber auch nochmal selbst wer am besten zu dir passt und triff dann deine eigene Entscheidung.
€ = Kostenpflichtig
Inv = Nur auf persönliche Anfrage oder Einladung

Mail:
- posteo.de (€)
- protonmail.com
- riseup.net (Inv)
- autistici.org (Inv)
- systemausfall.org (inv)
- systemli.org (Inv)
- so36.net (Inv)

- anonymousspeech.com (€)
- immerda.ch (Inv)
- free.de (Inv)

VPN:
- riseup.net
- ipredator.se (€)
- nordvpn.com (€)
- mullvad.net (€)
- securevpn.to (€)

Suche:
- duckduckgo.com
- startpage.com

Jabber/XMPP
- riseup.net (Inv)
- systemli.org
- systemausfall.org (Inv)
- so36.net (Inv)
- jabber.ccc.de

Eine ausführliche Liste von Software und Anbietern findest du bei PrismBreak. [53]

Resümee

Das wars. Hoffentlich konnte dir dieses Heft helfen. Beachte aber das hier bei weitem nicht alles abgedeckt wurde, es handelt sich eher um einen Rundumschlag um auf einen halbwegs ordentlichen Sicherheitsstandard zu kommen.

Falls du noch irgendwelche Fragen, Kritik oder Ergänzungen hast schreibe am besten eine PGP verschlüsselte E-Mail. Den Public-Key gibt es auf Anfrage. Die Adresse findest du auf der ersten Seite.

Falls du noch mehr zum Thema lesen willst empfehlen sich unter anderem die Kolumne „Get Connected“ der Datenschutzgruppe der RH Heidelberg, zu finden unter https://datenschmutz.de/gc/ und die Texte der Gruppe Capulcu, zu finden unter https://capulcu.blackblogs.org/. Außerdem kannst du unter https://privacy-handbuch.de noch eine Menge detaillierterer Informationen zu Anonymisierung, Verschlüsselung und Schutz vor Tracking nachlesen.

Vielen Dank an alle die bei der Erstellung des Hefts mitgeholfen haben und an alle die Ergänzungen einsenden und kommentieren. Solidarische Grüße an alle emanzipatorischen Gruppen und Einzelpersonen im Netz und in der analogen Welt.

Es folgen nun noch die Querverweise aus dem Text.

Links zum Thema

[1] Udo Vetter - Sie haben das Recht zu schweigen
https://youtu.be/3T-n1KH2GXU

[2] Rote Hilfe - Hausdurchsuchung. Was tun?
https://tinyurl.com/y7ddhvmw

[3] Rote Hilfe - Was tun wenn’s brennt?
https://tinyurl.com/y7b2hmjp

[4] Nachtmagazin - Überwachung durch Staatstrojaner
https://youtu.be/8REBKuFGfk8

[5] Chaos Computer Club analysiert Staatstrojaner
https://www.ccc.de/de/updates/2011/staatstrojaner

[6] Berlin hat den Staatstrojaner gekauft
https://tinyurl.com/y4a3vf9h

[7] FinFisher Hack
https://tinyurl.com/qj9zbvo

[8] HackingTeam Hack
https://tinyurl.com/onbq4re

[9] Wikipedia - Vorratsdatenspeicherung
https://de.wikipedia.org/wiki/Vorratsdatenspeicherung

[10] Polizei überwacht vor allem wegen Drogen
https://tinyurl.com/y5txu4d8

[11] Polizei überwacht erstmals weniger
http://tinyurl.com/y2xulr54

[12] Eraser
https://eraser.heidi.ie/

[13] wipe
http://lambda-diode.com/software/wipe/

[14] DBAN
https://dban.org

[15] VeraCrypt
https://www.veracrypt.fr/

[16] Anleitung VeraCrypt-Systemverschlüsselung
https://tinyurl.com/y7484om2

[17] Windows Upgrade bei Systemverschlüsselung
https://github.com/th-wilde/veracrypt-w10-patcher

[18] Anleitung VeraCrypt-Container
https://tinyurl.com/muvyjm2

[19] Anleitung Linux Verschlüsseln
https://tinyurl.com/h7emzgt

[20] Anleitung BIOS Passwort
https://www.wikihow.com/Set-a-BIOS-Password

[21] How to Encrypt your Android Phone
https://tinyurl.com/yax7xbcv

[22] GPG4Win
https://www.gpg4win.org/

[23] Thunderbird
https://www.thunderbird.net/de/

[24] Enigmail
https://enigmail.net/

[25] Why You Should Stop Using Telegram Right Now
https://tinyurl.com/jruf5mh

[26] Signal
https://www.signal.org/

[27] Jabber/XMPP
https://xmpp.org/software/clients.html

[28] Wikipedia - Gummischlauch-Kryptoanalyse
https://tinyurl.com/y8vohnez

[29] VeraCrypt - Plausible Deniability
https://tinyurl.com/y9xq76sr

[30] Keepass
https://keepass.info/

[31] KeepassRPC
https://keepass.info/plugins.html#keepassrpc

[32] Kee
https://www.kee.pm/

[33] Authy
https://www.authy.com/

[34] andOTP
https://github.com/andOTP/andOTP

[35] Decent Security
https://decentsecurity.com

[36] Tor
https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29

[37] Tor Browser
https://www.torproject.org/

[38] Tails
https://tails.boum.org/

[39] Whonix
https://www.whonix.org/

[40] VirtualBox
https://www.virtualbox.org/

[41] Whonix Images
https://www.whonix.org/wiki/VirtualBox/XFCE

[42] Qubes
https://www.qubes-os.org/

[43] IMSI-Catcher
https://de.wikipedia.org/wiki/IMSI-Catcher

[44] SnoopSnitch
https://opensource.srlabs.de/projects/snoopsnitch

[45] Darshak
https://github.com/darshakframework/darshak

[46] AIMSICD
https://tinyurl.com/jzjsedk

[47] Berliner Transparenzsystem
https://fts.berlin.de/

[48] Stille SMS
https://de.wikipedia.org/wiki/Stille_SMS

[49] Statistik Stille SMS
https://tinyurl.com/y9v5mfqv

[50] The Paddy Factor
https://tinyurl.com/y54jlqkq

[51] Codes, What Are They Good For?
https://tinyurl.com/y3y4dcwo

[52] 10 OPSEC Principles
https://operational-security.com/10-opsec-principles/

[53] Prism Break
https://prism-break.org/de/

[54] aTalk XMPP
https://atalk.sytes.net/

[55] uBlock
https://github.com/gorhill/uBlock/

[56] Capulcu Broschüre über Tails
https://tinyurl.com/y4wpfxdx

[57] Scrambled Exif
https://gitlab.com/juanitobananas/scrambled-exif

[58] RHZ 2018/4 Schwerpunkt Tipps für Aktivismus
https://tinyurl.com/y6k2sxzf

[59] SDelete
https://tinyurl.com/ydfg73l4

[60] Conversations XMPP
https://f-droid.org/en/packages/eu.siacs.conversations/

[61] Gajim XMPP Desktop Client
https://gajim.org

[62] F-Droid
https://f-droid.org

[63] Tox
https://qtox.github.io/

[64] Wire
https://wire.com/de/

[65] Jitsi
https://jitsi.org/

[66] VeraCrypt Hidden Operating System
https://tinyurl.com/sfldele

[67] Plausible Deniability With LUKS
https://tinyurl.com/j65spck